UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/075,194	02/12/2002	Klimenty Vainstein	2222.5390003	7090

26111 7590 04/28/2008

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
PALIWAL, YOGESH	
ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
04/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/075,194	VAINSTEIN ET AL.	
	Examiner	Art Unit	
	YOGESH PALIWAL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *1/10/08*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/29/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

- Applicant's amendment filed on 1/10/2008 has been entered. Applicant has amended claims 1, 21, 34, and 35. Currently claims 1-44 are pending in this application.

Docketing

1. Please note that the application has been re-docketed to different examiner. Please refer all future communications regarding this application to the examiner of record using the information supplied in the final section of the office action.

Response to Arguments

2. Applicant's arguments with respect to 35 U.S.C. 112 first paragraph rejection of claim 36 have been fully considered and are persuasive. The 35 U.S.C. 112, first paragraph rejection of claim 36 has been withdrawn.

3. Applicant's arguments with respect to U.S.C. 103(a) rejection of claims 1-35 have been considered but are moot in view of the new ground(s) of rejection.

4. Applicant's arguments with respect to U.S.C. 103(a) rejection of claims 36-44 have been fully considered but they are not persuasive for following reasons:

- Applicant argues: "The Examiner states at page 4 of the Office Action that at page 336 the Stallings reference teaches, through the use of "session keys," accessing a secured item through at most one local server at a time. However, the Examiner concedes Stallings does not teach or suggest permitting access based on information stored in an encrypted header of a secure item, but rather refers to Narasimhalu as allegedly teaching the use of a secret key to encrypt a secure item, and then storing the secret key in an encrypted header, which is then used to permit access. (Office Action, p. 4). However, even assuming, arguendo, that the

Examiner's statements of Narasimhalu and Stallings are correct, there is no teaching or suggestion of providing access to a secure item through a local server **based on the information stored** in an encrypted header of the secure item, as recited in claim 36. To the extent Narasimhalu permits access to a secure item based on information in a header, it does not control access through a particular one of a set of local servers. Further, neither Narasimhalu nor Stallings teach or suggest the transmission of, for example, the secret key of Narasimhalu to a local server in order to grant access to a secure item, nor any functionally similar behavior, as recited in claim 36."

- Applicant's arguments regarding claim 36 are not persuasive. Stallings does not explicitly discloses wherein, based on information stored in an encrypted header of a secure item a given requestor, permitted to access the secure item through one or more of said local servers. However, Narasimhalu clearly discloses wherein, based on information stored in an encrypted header of a secure item a given requestor, permitted to access the secure item (Fig. 2 and 4 in combination with page 5 lines 35-47) through one or more of a local server (See Fig. 1, numeral 10, "Information provider", secure item is provided through information provider which is interpreted as a server). Therefore, examiner maintains that the combination of Stallings and Narasimhalu still disclose all the limitations of claim 36 and thus the rejection is maintained.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill

in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 36 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings (Cryptography and Network Security) in view of Narasimhalu et al (EP 0672991 A2).

In reference to claim 36, Stallings teaches the Keberos system comprising: a central server having a server module that provides overall access control (Keberos authentication server page 333); and a plurality of local servers, each of said servers including a local module that provides local access control (last paragraph on page 333), wherein the access control, performed by said central server or said local servers, operates to permit or deny access requests to secured items by requestors (Kerberos authentication server Fig 11.2), and wherein a given requestor is only able to access secured items using only a single one of said local servers or the central server such that the given requestor can only access secured items through at most one of said local servers at a time even though the given requestor is permitted to access secure items through more than one of said local servers (page 336 Session keys).

Although Stallings discloses permitting access to a requestor, Stallings does not teach permitting access based on information stored in an encrypted header of a secure item.

Narasimhalu teaches a system and apparatus for controlling the dissemination of digital information. Narasimhalu discloses wherein, based on information stored in an encrypted header (secret key) of a secure item a given requestor, permitted to access the secure item (Fig. 2 and 4 in combination with page 5 lines 35-47) through one or more of a local server (See Fig. 1, numeral 10, “Information provider”, secure item is provided through information provider which is interpreted as a server).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to place access information in a header and encrypt the header as in Narasimhalu in the system of Stallings. One of ordinary skill in the art would have been motivated to do this because the system would allow for the control of the use of digital information (page 2 line 54 to page 3 line 2).

Claims 1-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sampson et al (6,339,423), hereinafter, "Sampson" in view of Boebert et al (5,502,766), hereinafter, "Boebert" and further in view of En-Seung et al. (US 6,892,306 B1), hereinafter, "En-Seung".

In reference ***to claims 1 and 34***, Sampson discloses a system and method comprising: (a) receiving, at a first server machine of the plurality of server machines (Fig. 2), an access request to access secure items from a user of a first client machine at a first location (column 4 lines 35-36), (b) authenticating the user of the first client machine at the first location (column 5 lines 30-45); (d) determining whether the user is permitted to gain access to secure items via the first location when said authenticating (b) and (c) are successful (column 4 line 62 to column 5 line 2) (e) permitting the user to gain access to secure items via the first server machine when said determining (d) determines that the user is permitted to gain access to secure items from the first location (Fig 3 A and B parts 318-338), and (f) preventing the user to gain access to secure items via the first server machine when said determining (e) determines that the user is not permitted to gain access to secure items from the first location (Fig 3A and B parts 318-332).

Although the system of Sampson discloses and authentication process for the user, the system does not disclose (c) authenticating the first client machine.

Boebert discloses a system for providing the secure transfer and sharing of data via a local area network (abstract). The system comprises an identification and authentication process for the user and the client machine (column 4 lines 26-35).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Sampson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area.

Sampson and Boebert do not teach retrieving at the first server machine a user key permitting access to an encrypted header of the secured item, the encrypted header including access rules for the secured item.

En-Seung discloses, retrieving at a server machine a user key permitting access to an encrypted header of the secured item, the encrypted header including access rules for the secured item (See Fig. 19 and also Column 3, lines 14-32).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to place access information in a header and encrypt the header with a user key as in En-Seung in the system of Stallings. One of ordinary skill in the art would have been motivated to do this because the system would provide a more secure cryptograph and process for transmitting information to a terminal of a user who has requested the information (See Column 2, lines 55-57).

In reference to ***claims 21 and 35****,* Sampson discloses a system and method comprising: receiving, at a first server machine of the plurality of server machines (Fig. 2), an access request to

access secure items from a user of a first client machine at a first location (column 4 lines 35-36), authenticating the user of the first client machine at the first location (column 5 lines 30-45); retrieving access privileges associated with the user (column 5 lines 38-46); determining whether the user is permitted to gain access to secure items via the first location when said authenticating are successful (column 4 line 62 to column 5 line 2) permitting the user to gain access to secure items via the first server machine when said determining determines that the user is permitted to gain access to secure items (Fig 3 A and B parts 318-338), and preventing the user to gain access to secure items via the first server machine when said determining determines that the user is not permitted to gain access to secure items from the first location (Fig 3A and B parts 318-332).

Although the system of Sampson discloses and authentication process for the user, the system does not disclose authenticating the first client machine.

Boebert discloses a system for providing the secure transfer and sharing of data via a local area network (abstract). The system comprises an identification and authentication process for the user and the client machine and determining whether user is permitted access from the location (column 4 lines 26-35).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Sampson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

Sampson and Boebert do not teach retrieving at the first server machine a user key permitting access to an encrypted header of the secured item, the encrypted header including access rules for the secured item.

En-Seung discloses, retrieving at a server machine a user key permitting access to an encrypted header of the secured item, the encrypted header including access rules for the secured item (See Fig. 19 and also Column 3, lines 14-32).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to place access information in a header and encrypt the header with a user key as in En-Seung in the system of Stallings. One of ordinary skill in the art would have been motivated to do this because the system would provide a more secure cryptograph and process for transmitting information to a terminal of a user who has requested the information (See Column 2, lines 55-57).

In reference to ***claim 2***, although the system of Sampson discloses and authentication obtaining access privileges associated with the user (column 4 line 62 to column 5 line 2), Sampson does not disclose a system of authentication wherein said determining comprises: to determine at least permitted locations for the user; and (d2) determining whether the user is permitted to gain access to secure items from the first location based on the permitted locations associated with the user.

Boebert discloses a system for authentication wherein the determining comprises obtaining access privileges associated with the user to determine at least permitted locations for the user; and determining whether the user is permitted to gain access to secure items from the first location based on the permitted locations associated wit the user (column 4 lines 27-45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Sampson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to ***claim 3****,* wherein, when permitted by said permitting (e), the user gains access to secure items from the first location via the first client machine and the first server machine.

Although the system of Sampson discloses and authentication process for the user, the system does not disclose authenticating the first client machine.

Boebert discloses a system for providing the secure transfer and sharing of data via a local area network (abstract). The system comprises an identification and authentication process for the user and the client machine and determining whether user is permitted access from the location (column 4 lines 26-35).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Sampson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to ***claim 4****,* wherein, when permitted by said permitting (e), the user gains access to secure items from the first location via the first client machine and the first server machine.

Although the system of Sampson discloses and authentication process for the user, the system does not disclose authenticating the first client machine.

Boebert discloses a system for providing the secure transfer and sharing of data via a local area network (abstract). The system comprises an identification and authentication process for the user and the client machine and determining whether user is permitted access from the location (column 4 lines 26-35).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Sampson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to ***claims 5, 22, and 24****,* wherein said method comprises the acts of: (g) preventing the user from gaining access to secure items via any of the server machines other than the first server machine when said determining (d) determines that the user is permitted to gain access to secure items from the first location.

Although the system of Sampson discloses and authentication process for the user, the system does not disclose authenticating the first client machine.

Boebert discloses a system for providing the secure transfer and sharing of data via a local area network (abstract). The system comprises an identification and authentication process for the user and the client machine and determining whether user is permitted access from the location (column 4 lines 26-35). The user is only permitted to access the resource from a particular location

therefore since the other locations are not permitted to access the resource the no other server will permit access.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Sampson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to ***claims 6 and 23***, wherein said determining (d) comprises determining whether the user is permitted to gain access to secure items via the first client machine and the first server machine, and wherein said permitting (e) operates to permit the user to gain access to secure items via the first client machine and the first server machine when said determining (d) determines that the user is permitted to gain access to secure items via both the first client machine and the first server machine.

Although the system of Sampson discloses and authentication process for the user, the system does not disclose authenticating the first client machine.

Boebert discloses a system for providing the secure transfer and sharing of data via a local area network (abstract). The system comprises an identification and authentication process for the user and the client machine and determining whether user is permitted access from the location (column 4 lines 26-35).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the

system of Boebert in that authentication process of Sampson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to ***claim 7,*** wherein said determining comprises determining whether the user is permitted to gain access to secure items via the first server machine, and wherein said permitting operates to permit the user to gain access to secure items via the first server machine when said determining determines that the user is permitted to gain access to secure items via the first server machine (Fig 2 and 3).

In reference to ***claim 8***, wherein said determining (d) comprises determining whether the user is permitted to gain access to secure items via the first client machine, and wherein said permitting (e) operates to permit the user to gain access to secure items via the first client machine when said determining (d) determines that the user is permitted to gain access to secure items via the first client machine (Fig 2 and 3).

In reference to ***claim 9,*** wherein said method comprises the acts of: (g) preventing the user from gaining access to secure items via any of the server machines other than the first server machine when said determining (d) determines that the user is permitted to gain access to secure items from the first location.

Although the system of Sampson discloses and authentication process for the user, the system does not disclose authenticating the first client machine.

Boebert discloses a system for providing the secure transfer and sharing of data via a local area network (abstract). The system comprises an identification and authentication process for the

user and the client machine and determining whether user is permitted access from the location (column 4 lines 26-35).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Sampson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to ***claims 10 and 25***, wherein said preventing (g) of the user to gain access to secure items via any of the other server machines comprises reconfiguring at least any of the other server machines that previously permitted the user to gain access to secure items therethrough.

Although Sampson discloses preventing the user to gain access to secure items via any of the other server machines, Sampson does not disclose preventing access to the server machine by reconfiguring at least any of the other server machines that previously permitted the user to gain access. Boebert also does not disclose the reconfiguration. However, Boebert discloses controlling access to the resource using keys.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to revoke the key from the user when the user is no longer permitted access in the system of Boebert. One of ordinary skill in the art would have been motivated to do this because when the user is no longer permitted to access the resource revoking the key would discourage fraudulent activities.

In reference to ***claims 11 and 26****,* wherein said permitting of the user to gain access to secure items via the first server machine comprises reconfiguring the first server machine to permit access by the user to secured items via the first server machine.

Although Sampson discloses preventing the user to gain access to secure items via any of the other server machines, Sampson does not disclose preventing access to the server machine by reconfiguring at least any of the other server machines that previously permitted the user to gain access. Boebert also does not disclose the reconfiguration. However, Boebert discloses controlling access to the resource using keys.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to revoke the key from the user when the user is no longer permitted access in the system of Boebert. One of ordinary skill in the art would have been motivated to do this because when the user is no longer permitted to access the resource revoking the key would discourage fraudulent activities.

In reference ***claim 12*** wherein said determining (d) comprises: obtaining access privileges associated with the user to determine at least permitted locations for the user; and determining whether the user is permitted to gain access to secure items from the first location based on the permitted locations associated with the user.

Although the system of Sampson discloses and authentication obtaining access privileges associated with the user (column 4 line 62 to column 5 line 2), Sampson does not disclose a system of authentication wherein said determining comprises: to determine at least permitted locations for the user; and (d2) determining whether the user is permitted to gain access to secure items from the first location based on the permitted locations associated with the user.

Boebert discloses a system for authentication wherein the determining comprises obtaining access privileges associated with the user to determine at least permitted locations for the user; and determining whether the user is permitted to gain access to secure items from the first location based on the permitted locations associated wit the user (column 4 lines 27-45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Sampson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to ***claims 13 and 27*** wherein said permitting of the user to gain access to secure items via the first server machine comprises reconfiguring the first server machine to permit access by the user to secured items via the first server machine (column 5 lines 475-60).

In reference to ***claims 14 and 28*** wherein each of the secure items is a secured file, the secured file having a format that comprises a header including security information as to who and how the secure item can be accessed, an encrypted data portion including data of the secure file encrypted with a file key according to a predetermined cipher scheme, and wherein the header is attached to the encrypted data portion to generate the secured file.

Sampson does not disclose an encrypted data portion. However Boebert discloses each of the secure items is a secured file, the secured file having a format that comprises a header including security information as to who and how the secure item can be accessed, an encrypted data portion including data of the secure file encrypted with a file key according to a predetermined cipher

scheme, and wherein the header is attached to the encrypted data portion to generate the secured file (Fig. 12).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Sampson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to ***claims 15 and 29***, wherein the security information in the header of the secured file facilitates the restricted access to the secured file.

Boebert discloses a system wherein the security information in the header of the secured file facilitates the restricted access to the secured file (part 90 Fig. 8).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Sampson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to ***claim 16***, wherein the security information in the header of the secured file points to or includes the access rules and a file key.

Boebert discloses the security information in the header of the secured file points to or includes the access rules and a file key (Fig. 10).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Sampson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to ***claims 17 and 30***, wherein the security information is encrypted with a user key associated with a user.

Boebert discloses the security information is encrypted with a user key associated with a user (Fig. 12).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Sampson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to ***claims 18 and 31***, wherein the security information includes the file key and access rules to the restricted access to the secured file.

Boebert discloses security information includes the file key and access rules to the restricted access to the secured file (Fig. 16).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the

system of Boebert in that authentication process of Sampson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to ***claims 19 and 32*** wherein the file key is retrieved to decrypt the encrypted data portion in the secured file when access privilege of the user is within access permissions by the access rules.

Boebert discloses retrieving the file key to decrypt the encrypted data portion in the secured file when access privilege of the user is within access permissions by the access rules (Fig. 16).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the system of authenticating the client machine as well as the human user as in the system of Boebert in that authentication process of Sampson. One of ordinary skill in the art would have been motivated to do this because it enables the implementation of sophisticated security policies by the Secure Computer such as the user may be authorized to access engineering drawings, but only form terminals located inside the engineering area (column 4 lines 35-45).

In reference to ***claims 20 and 33***, wherein the access rules are expressed in a markup language. Sampson and Boebert do not disclose the access rules are expressed in a markup language. However at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a markup language to express the access rules. One of ordinary skill in the art would have been motivated to do this because markup languages are a set of codes in a text file that instruct a computer how to format it on a printer or video display or how to index and link its contents and therefore it would determine how to index the content based on the access rules.

Claims 37-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Narasimhalu as applied to claim 36 above, and further in view of Skarbo et al (6,317,777).

In reference ***to claim 37***, wherein said access control system couples to an enterprise network to restrict access to secured files stored therein.

Stallings discloses the authentication to access to a service, however Stallings does not disclose access control system couples to an enterprise network to restrict access to secured files stored therein.

Skarbo discloses a document-collaboration videoconferencing system between a first and a second conference attendee (abstract). The system comprises access control system couples to an enterprise network to restrict access to secured files stored therein (Fig. 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art that the service provided by the server after authentication should be an enterprise network to restrict access to secured files stored therein as in the system taught by Skarbo in the server disclosed by Stallings. One of ordinary skill in the art would have been motivated to do this because the system would reliably deliver conferencing data to conference participants (Skarbo column1 lines 45-50).

In reference to ***claim 38***, wherein the access requests are at least primarily processed in a distributed manner by said local servers (Fig. 11.2).

In reference to ***claim 39***, wherein when the access requests are processed said local servers, the requestors gain access to the secured files without having to access said central server (Fig. 11.2).

In reference to ***claim 40***, wherein the local module can be a copy of the server module so any of the local modules can operate independent of said central server and other of said local servers (Fig. 11.2).

In reference to ***claim 41*****,** wherein the local module can be a subset of the server module (Fig. 11.2).

In reference to ***claim 42*****,** wherein access permissions for said local servers can be dynamically configured to pass a requestor from one of said local servers to another of said local servers, thereby enabling access control to be performed by the another of said local servers such as when the location of the requestor changes (Fig. 11.2 multiple kerberi).

Claims 43-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Narasimhalu and Skarbo as applied to claim 37 above, and further in view of Pensak (6,449,721 B1).

In reference to ***claims 43-44***, wherein the secured files are secured by encryption.

Although Stallings discloses the exchange of session keys, Stallings does not expressly disclose that the service is secured by encryption.

Pensak discloses secured files are secured by encryption (Fig. 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to secure the files by encryption as in Pensak in the system of Stallings. One of ordinary skill in the art would have been motivated to do this because encryption is a process for encoding data that prevents unauthorized access especially during transmission.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YOGESH PALIWAL whose telephone number is (571)270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Y. P./
Examiner, Art Unit 2135

/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135